Amendments to the Specification:

Please amend the specification as follows:

Please replace the paragraph bridging pages 7 and 8 (page 7, line 22 to page 8, line 14, with the following rewritten paragraph:

The use of a key in the process of distributing secure content to a subscriber will now be described briefly with reference to Fig. 3. The process is initiated by transaction 300 with receipt by the subscriber of a request 302 for a subscription from a would-be subscriber. The request at this stage is likely to include some form of payment, or promise to pay. Given the need for anonymity of subscribers, the processing of any payment at the server is likely to be dealt with first, and successful payment processing will simply yield an indication to the key management program 110 that the requesting subscriber is entitled to a given level of content provision, e.g., "GOLD" for a given period of time. The key management program then allocates a key to the requesting subscriber at operation 304, and this key is sent back to the subscriber at transaction 306 as part of a cookie 308, which includes the key, here represented as #D2, and a time to live DDMMYYYY for this key, this being the date when the subscription paid for in the payment step expires. It should be noted as this point that, unlike the majority of cookies usually passed to clients from servers, in the present example the cookie 308 does not given any indication of the identity of the requesting subscriber, and other than during the payment process, which is performed entirely separately in the key allocation process, no data identifying the subscriber has been received by the server. [[NB]] In a modification, payment may be made by the subscriber to a trusted third party, who, once payment has been made, then simply passes data indicating the manner in which the client may be contacted to the server for the allocation of a key to that subscriber. Upon receipt of the key #D2, the subscriber then stores this key securely at operation 310. When the subscriber then wants to gain access to the content 100 in respect of which they have subscribed, the cookie 308 containing the key #D2 is retrieved at operation 312 and sent [[to]] together with a request to access the content in transaction 314. When such a request

is received, the server extracts the key #D2 from the cookie, and using the key #D2 authenticates the request at operation 316.

Please replace the paragraph bridging pages 8 and 9 (page 8, line 32 to page 9, line 19, with the following rewritten paragraph:

The specific process of authentication involves firstly location of the key #D2 within the tree of Fig. 2. As mentioned above, each key includes an indication of [[the]] its address within the tree in the form of a path from the root key A0, so that in the present example, the key #D2 will implicitly contain data indicative of the path A0-B1-D2. Once the node or address D2 within the tree has been located, the key #D2 is simply matched with the key at that address, and if they are the same then the key #D2 is assumed to be genuine. Authentication of the level of content provision may be performed in a number of ways. In one embodiment a mapping is made of each key issued from tree to the level of content provision for which the subscriber has paid, so that upon receipt and authentication of the key, the authenticated key is then mapped to the content level, and the content level indicated by this mapping is matched with the requested content level. If both the key and the requested content level are authenticated at operation 316, the server then retrieves the requested content and encrypts it with the subscriber's key at operation 317, before dispatching the encrypted content to the subscriber at transaction 318. The subscriber then retrieves their key from secure storage, and uses the key to decrypt the content at operation 320. If, at some later stage, the subscriber no longer wishes to subscribe, they may request cancellation of their subscription at transaction 322, and following receipt of such a cancellation request, the server inactivates the key to prevent the now-cancelled subscriber from gaining access to the content without paying for it.

Please replace the paragraph bridging pages 11 and 12 (page 11, line 26 to page 12, line 3, with the following rewritten paragraph:

Referring once again to Fig. 2, consider a scenario where the subscription for the key of node D2 has just lapsed. The opportunity cost of invalidating the key of node D2 is, as mentioned above, a total of seven keys, which is fractionally less than 20% of the total number of keys in the tree. The cost of invalidation of the key #D2 can thus be justifiably be quantified as approximately 20% of the cost of providing a new tree (including the distribution of new keys to existing subscribers). However, this assessment is based on the absolute cost as a proportion of a new tree, but if a significant number p of total available keys N of a new tree have already been invalidated, then as a proportion of the remaining keys the opportunity cost is that much greater, i.e., 0.2N/[N-p]. To be added to this is the cost of reconfiguration of at least a part of all the other keys in tree to the extent that they share ancestral keys with **[[**D2**]]** key #D2, and distribution of these reconfigured key elements to their subscribers.